Security Update

David Crooks

on behalf of Ian Neilson and NGI UK Security Team

GridPP37, September 2016

Overview

- NGI UK Security Team

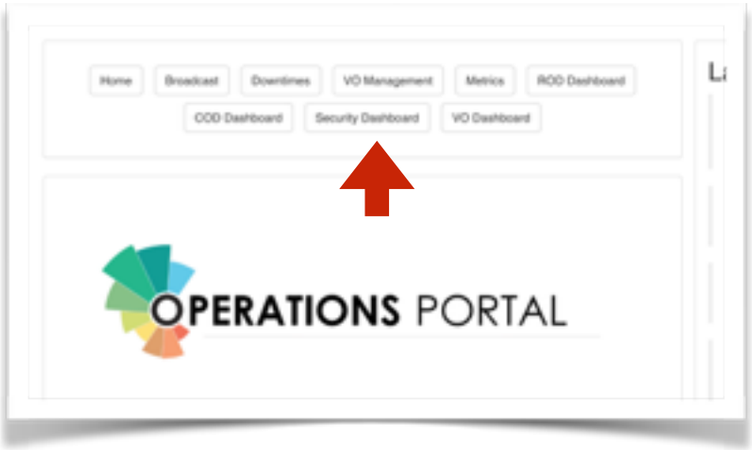
- WLCG Security Working Groups

NGI UK Security Team

- Ian Neilson, Jeremy Coles, Ian Collier, David Crooks, Linda Cornwall, Alessandra Forti, Rob Harper, Dave Kelsey
- ukngi-security@cern.ch
- ~ Twice monthly phone conferences

Responsibilities

- Support for security officer + on duty
  - Security Dashboards
    - https://pakiti.egi.eu
    - https://operations-portal.egi.eu



- Team supports incident handling + communications with EGI CSIRT

- Overlap of membership with EGI CSIRT

Last ~6 months

- Several broadcasts from SVG (see Dave Kelsey's talk), 2 critical
  - Critical advisories treated differently as well as being more urgent
  - https://wiki.egi.eu/wiki/SVG:Advisories
  - Monitored in Ops calls and through other means
- A couple of other issues in the UK
- Attended by security team for support

UK SRM ARGUS ban testing

- Presented prelim test @GridPP36.
- Retested SRM for OPS VO Jul/Aug

- 2 certificate DNs registered in VO gridpp (ops?)
  - /C=UK/O=eScience/OU=CLRC/L=RAL/CN=ian neilson (ukngi sec)
  - /C=UK/O=eScience/OU=CLRC/L=RAL/CN=ian neilson
  - Get one banned (used to test “emergency ban” ☺)
- Generate lists of target resources
  - *e.g. lcg-infosites --vo gridpp se*
- Scripts to run jobs
  - SEs: *gfal-copy* local -> remote
    - Job fails to submit with banned cred.

SRM Argus Testing

- Test SRM endpoints registering support for OPS VO
- 17 sites (with 39 endpoints)
- 12 “failures” to ban notified
  - 11 acknowledged email notification
  - 8 corrected configuration
  - 1 ongoing & 1 failed to acknowledge
  - 1 can’t be configured: Castor needs a manual procedure ☹
- Conclusions
  - No reports of significant difficulty with configuration or instability/ performance hits.
  - Some “I though it was” implies some use to the exercise
  - Rather labour intensive (65 emails & 36 jobs in the folder)

SRM ARGUS Testing

- Thanks for all co-operation
- Will repeat again (maybe early next year) or on demand by sites.

- Coming-up: CSIRT communications challenge.

WLCG security working groups

- Traceability & Isolation (Vincent Brillault)

- Security Operations Centres (Liviu Vâlsan/myself)

Traceability & Isolation

- "Explore new traceability and isolation paradigms, propose a new model taking advantage of new technologies and VO frameworks while keeping full trustworthy traceability and isolation of users actions."

- Two main strands
  - Information
  - Technology

- UK represented by: *Ian Collier, David Crooks, Alessandra Forti, Andrew Lahiff, Andrew McNab, Ian Neilson*

Information

- What information are VOs gathering - glexec?
- Current VO traceability & isolation
- Cost of identifying a job

Technology

- (User) Namespacing/containers/cgroups…
- Ongoing investigation into unprivileged namespace support in RHEL 7.x

Security Operations Centres

- Analytics for security

- “Establish a clear set of desired data outputs and necessary inputs.

- Create a scalable reference design applicable for a range of sites by examining current and prospective SOC projects & tools.”

- UK represented by: *Ian Collier, David Crooks, Joe Dyer, Dave Kelsey, Andrew Lahiff, Ian Neilson, Raul Lopes, Oliver Smith, Andrew Washbrook*

Strategy

- Start with specific tools and grow our understanding and requirements

- New area of work - challenges include engaging with all the appropriate security teams and stakeholders

Plan & actions

- MISP Threat Intelligence sharing
  - RAL, Edinburgh, Glasgow
- Bro Network Security Monitor
  - Brunel, Durham
- Metron Security Operations Centre
  - Use as reference design

Other tools

- ZNeTS2
- Network capture & analysis tool
- Used widely in French labs.

Summary

- NGI UK Security Team provides support and communication with the GridPP community
- WLCG Working Groups are exploring security issues in new virtualised landscape
- Lots of work to do, extra help always welcome

Contacts

- NGI UK Security team:
  - ukngi-security@cern.ch
- Traceability & Isolation:
  - wlcg-traceability-isolation-wg@cern.ch
- SOC:
  - wlcg-soc-wg@cern.ch